UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,788	08/31/2001	Alfonso De Jesus Valdes	10454-022001/P-4190-4	1821

52197 7590 03/18/2010

Wall & Tong, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SHREWSBURY, NJ 07702

EXAMINER	
SHERR, CRISTINA O	

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
03/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/944,788	VALDES ET AL.	
	Examiner	Art Unit	
	CRISTINA SHERR	3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) *3-6,9-12,15-30* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,7,8,13 and 14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/17/09*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to Applicant's Amendment filed December 14, 2009. Claims 1-30 are pending in this case. Claims 1, 2, 7, 8, 13, and 14 are under examination. Claims 1, 7, and 8 are currently amended.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on September 17, 2009 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

3. Applicant's arguments filed December 14, 2009, with respect to the section 101 rejection of claims 1 and 2, as currently amended, have been fully considered but they are not persuasive.

4. Specifically, regarding claim 1, as currently amended, the device or machine represents mere extra-solution activity. The various steps in claim 1 can be reasonably interpreted as being performed by a person alerting another person via a shout, for example, or via mental steps in comparing one alert with another. Further, no material is being changed to a different state. For these reasons, independent claim 1 and its dependent claim 2 are rejected under section 101.

5. Applicant's arguments, see Remarks, filed December 14, 2009, with respect to the section 101 rejection of claims 7, 8, 13, and 14 as currently amended, have been fully considered and are persuasive. The section 101 rejection of claims 7, 8, 13, and 14 has been withdrawn.

6. Applicant's arguments filed December 14, 2009, with respect to the section 102 rejections of the claims, as currently amended, have been fully considered but they are not persuasive.

7. Applicant argues, regarding claims 1, 7, and 13, that nothing in the cited prior art teaches, discloses or suggests comparison of an alert in order to classify the alert.

8. Examiner respectfully disagrees and directs attention to Nine, col 8 ln 35-61, where the receiver receives a ticket or alert, parses the ticket and uses the information in the ticket in order to decide where to place the pending ticket according to its features, and who to notify depending on how the ticket has been classified.

9. Applicant argues, regarding claims 1, 7, and 13, that nothing in the cited prior art teaches, discloses or suggests examining the features of an alert, or of the need to update a threshold similarity requirement or a similarity expectation for the features of the alert to the one or more alert classes.

10. Examiner respectfully disagrees and directs attention to Nine, at, e.g. col 9 ln 22-40, where information is extracted from a ticket or alert file, to detect certain problems, and all the tickets with similar features are located in order to detect patterns, thereby creating a new group or classification according to the pattern.

Claim Rejections - 35 USC § 101

11. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

12. Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

13. Claims 1-2 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter

14. In this case, claims 1-2 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Based on Supreme Court precedent (See also *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1876)) and recent Federal Circuit decisions, a §101 process must (1) be tied to a particular apparatus or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In addition, the tie to a particular apparatus, for example, cannot be mere extra-solution activity. See *In re Bilski*, 88 USPQ2d 1385 (Fed. Cir. 2008). To meet prong (1), the method step should positively recite the other statutory class (the thing or product) to which it is tied. This may be accomplished by having the claim positively recite the machine that accomplishes the method steps. Alternatively or to meet prong (2), the method step should positively recite identifying the material that is being changed to a different state or positively recite the subject matter that is being transformed.

15. Specifically, regarding claim 1, the device or machine represents mere extra-solution activity, as part of a preamble. The various steps in claim 1 can be reasonably interpreted as being performed by a person alerting another person via a shout, for

example, or via mental steps in comparing one alert with another. Further, no material is being changed to a different state.

16. Additionally, in light of the amendment, it appears that Applicant did not feel claim 1 was sufficiently statutory. Applicant's newly-added language, however, as proposed "fix" represents mere extra-solution activity. Hence, the claim is directed to non-statutory subject matter.

17. For these reasons, independent claim 1 and its dependent claim 2 are rejected under section 101.

Claim Rejections - 35 USC § 102

18. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

19. Claims 1, 2, 7, 8, 13, and 14 are rejected under 35 U.S.C. 102(a) as being anticipated by Nine et al (US 6,560,611).

20. Regarding claims 1, 7, and 13 –

21. Nine discloses in an intrusion detection system (abs, col 2 ln 65-67) that includes a plurality of sensors (e.g. col 3 ln 1-5) that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features (col 4 ln 52-55), the method comprising the steps of:

(a) receiving a new alert (called “message” at col 3 ln 25-30 or “ticket” at col 3 ln 15-20, col 5 ln 32-34, col 7 ln 47-50, col 7 ln 63-col 8 ln 9);

(b) identifying a set of similar features shared by the new alert and one or more existing alert classes (e.g. col 3 ln 12-20, col 8 ln 35-42);

(c) updating a threshold similarity requirement for one or more features (e.g. col 5 ln 50-col 6 ln 10, col 9 ln 22-40);

(d) updating a similarity expectation for one or more features (e.g. col 5 ln 50-col 6 ln 10, col 9 ln 30-35);

(e) comparing the new alert with one or more alert classes, and either:

(f 1) associating the new alert with the existing alert class that the new alert most closely matches (col 7 ln 22-46, col 5 ln 32-37, col 8 ln 35-42); or

(f 2) defining a new alert class that is associated with the new alert (col 9 ln 5-40), wherein at least one of: the receiving, the identifying, the updating a threshold similarity, the updating a similarity expectation, the comparing, the associating, or the defining is performed by a processor. (col 3 ln 1-20)

22. Regarding claims 2, 8, and 14 –

23. Nine discloses the method of claim 1 further comprising the step (a) of passing each existing alert class through a transition model to generate a new prior belief state for each alert class (e.g. col 5 ln 60- col 6 ln 10, col 9 ln 22-40).

24. As above, although Nine discloses messages rather than “alerts”, the said messages are the functional equivalents of alerts, where generally, the disclosure of Nine may be adapted by one of ordinary skill in the art to obtain the instant application.

25. Claims 7 and 8 are alternatively rejected under 35 U.S.C. 102(a) as being anticipated by Baggon et al (US 4,667,317).

26. Claims 7 and 8, as currently amended, recite a computer readable storage medium as in Baggon (e.g. abstract).

27. In this case, the program on the computer readable storage medium in claim 7 is not actually causing anything to happen. Thus, it is nonfunctional descriptive material, and as such does not further distinguish the claims from the prior art. *In re Gulack*, 217 USPQ 401 (Fed. Cir. 1983), *In re Ngai*, 70 USPQ2d (Fed. Cir. 2004), *In re Lowry,* 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.01 II.

28. It is suggested that amending the claims to read "program causes a computer (or other appropriate device) to perform the steps of . . .", would make the claims distinguishable from a generic computer readable medium with data.

Conclusion

29. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

30. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

31. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CRISTINA SHERR whose telephone number is (571)272-6711. The examiner can normally be reached on 8:30-5:00 Monday through Friday.

32. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin L. Hewitt, II can be reached on (571)272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

33. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CRISTINA OWEN SHERR
Examiner
Art Unit 3685

/Calvin L Hewitt II/
Supervisory Patent Examiner, Art Unit 3685